TX-RAMP Overview

Matt Kelly
Deputy CISO – Policy & Governance

Webinar Information

- Presentation portion of the session will be recorded and available with slides on the DIR website.

- Attendance is at capacity for the platform.

- Questions/answer session after presentation.

- Type questions into the chat at any time.

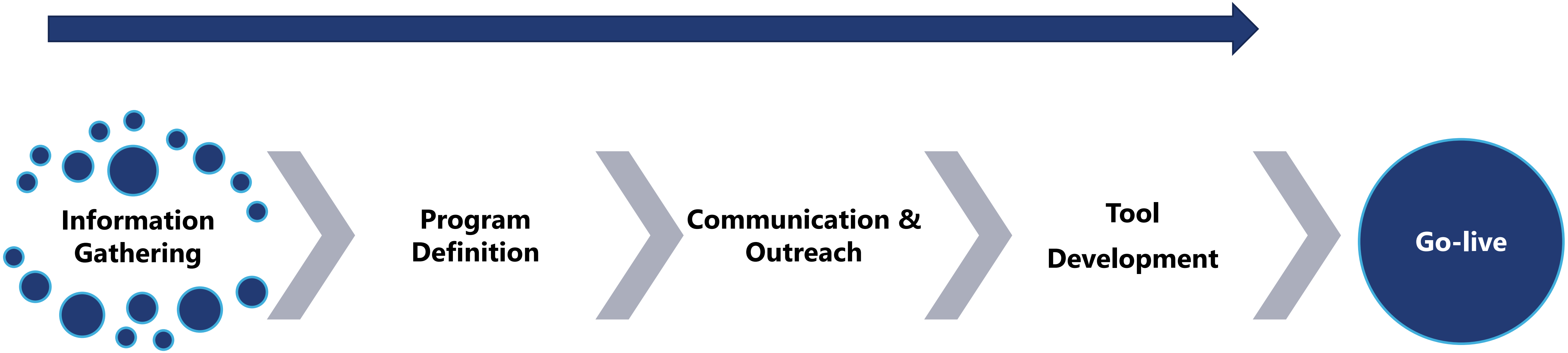
https://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp

Agenda

- Background & Overview
- Program Scope
- Certification Levels
- Other RAMPs
- TX-RAMP Assessment
- Continuous Monitoring
- Additional Information
- Questions & Answers

TX-RAMP Overview

Program Implementation Process



Information Gathering

- Usage Survey
- Vendor List
- Other RAMPs

Program Definition

- Develop Rule
- Assessment Levels/Controls
- Processes & Documentation

Communication & Outreach

- Customer Outreach
- Vendor Outreach

Tool Development

- Acquisition
- Configuration
- Testing

Go-live

- Tool Production Launch
- Data Collection
- Assessment & Certification

~Currently finalizing assessment questionnaires and SPECTRIM configuration~

SPECTRIM training webinar to be scheduled in near future

Texas Risk & Authorization Management Program

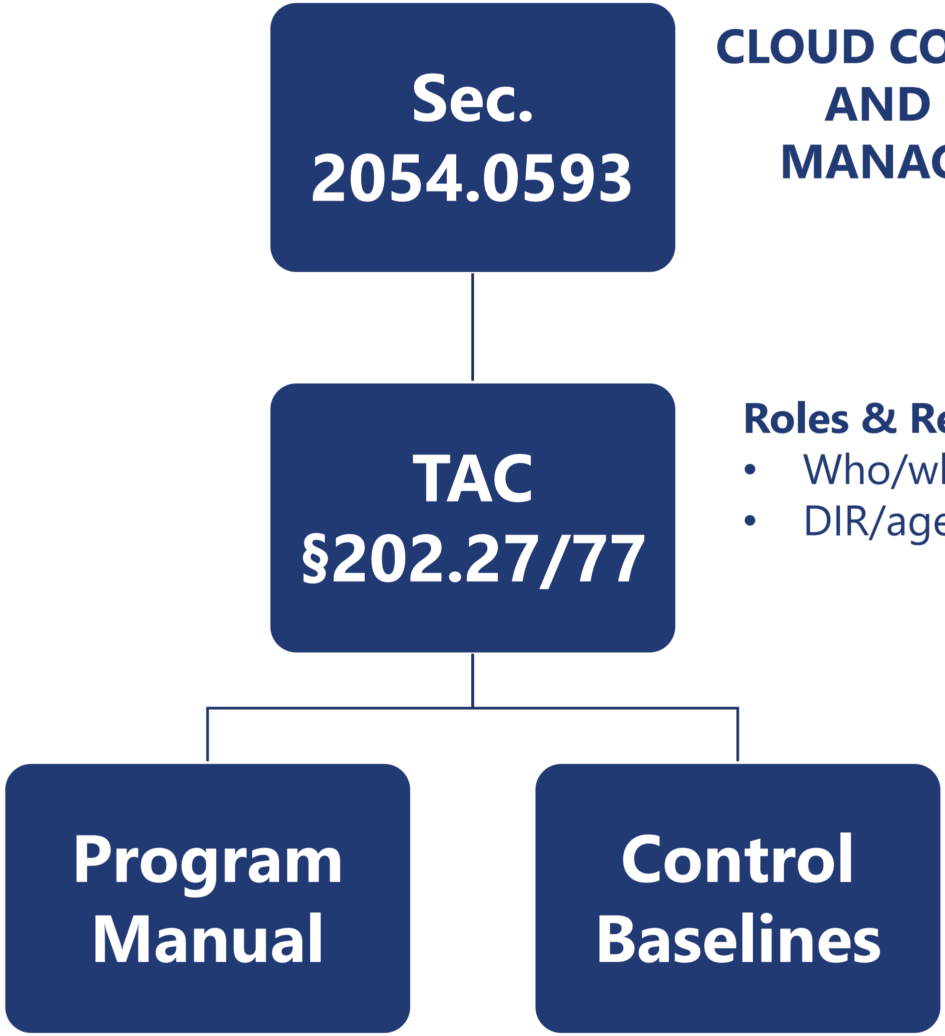
- **What is it?**
  - A framework for collecting information about cloud services security posture and assessing responses for compliance with required controls and documentation.

- **What does this apply to?**
  - Contracts for cloud services that store, process, or transmit agency data entered in, or renewed, on or after Jan 1, 2022.

- **Who does this apply to?**
  - Organizations subject to information security requirements of Government Code Chapter 2054:
    - State Agencies, Public Institutions of Higher Education, and Public Community Colleges.

https://dir.texas.gov/information-security/security-policy-and-planning/tx-risk-authorization-management-program-RAMP

Program Structure



Sec. 2054.0593

CLOUD COMPUTING STATE RISK AND AUTHORIZATION MANAGEMENT PROGRAM

TAC §202.27/77

Roles & Responsibilities

- Who/what is subject to the program
- DIR/agency/vendor responsibilities

Program Manual

Details certification process

- How to begin certification
- Decision-tools for baseline selection
- What information is needed

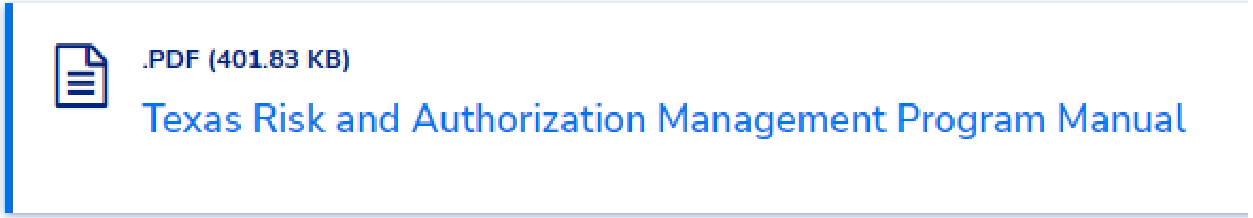
Control Baselines

Specifies applicable controls

- TX-RAMP Level 1
- TX-RAMP Level 2

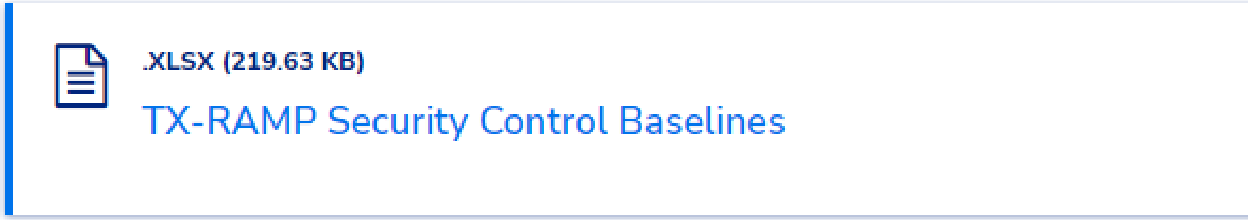
TX-RAMP Webpage

https://dir.texas.gov/tx-ramp



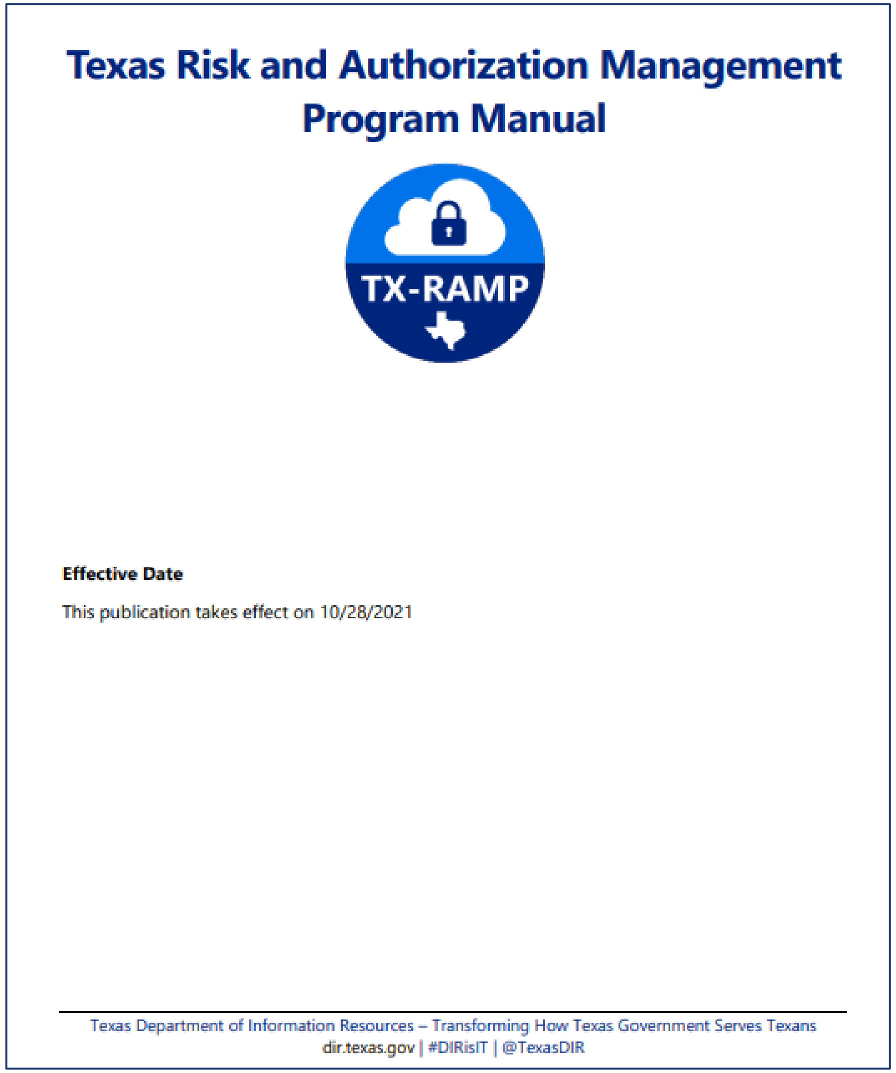
.PDF (401.83 KB)

Texas Risk and Authorization Management Program Manual



.XLSX (219.63 KB)

TX-RAMP Security Control Baselines



Texas Risk and Authorization Management Program Manual

Effective Date

This publication takes effect on 10/28/2021

Texas Department of Information Resources – Transforming How Texas Government Serves Texans
dir.texas.gov | #DIRisIT | @TexasDIR

TX-RAMP Scope

Cloud Computing – NIST SP 800-145

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Out of Scope – Categories & Characteristics

- Consumption-focused (advisory/research)
- Graphic Design/Illustration
- GIS/Mapping
- Email/Notification Distribution
- Social Media
- Survey/Scheduling
- LMS/Training
- Accreditation/Compliance Requirements
- Low-Impact SaaS

Provided that the cloud computing service <u>does not:</u>

1.) create, process, or store confidential state-controlled data (except as needed to provide a login capability, e.g. username, password, email) or

2.) connect with agency systems or networks that create, process, or store confidential state-controlled data such that any security incident might affect such systems or networks.

Low-Impact SaaS

- ✓ Meet definition of SaaS (NIST-SP 800-145)
- ✓ Does not contain PII except as needed to login
- ✓ No confidential information
- ✓ Low-impact information resource (per TAC 202)
- ✓ Operates on TX-RAMP certified IaaS/PaaS

Agencies should document cloud services designated as out-of-scope in accordance with agency policies.

Certification Levels

Certification Levels

Nonconfidential Data – Information that is not required to be or may not be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

- **TX-RAMP Level 1**
  - Nonconfidential data **OR**
  - Low-impact information resources
- **TX-RAMP Level 2**
  - Confidential information **AND**
  - Moderate or high-impact information resources
- **TX-RAMP Provisional**
  - Level agnostic
  - Agency-sponsored or 3rd party assessment review
  - Valid for 18 months

Impact Determination

Information Resources whose loss of confidentiality, integrity, or availability could be expected to have…

Low Impact	Moderate Impact	High Impact
• a limited adverse effect on operations, assets, or individuals.	• a serious adverse effect on operations, assets, or individuals.	• a severe or catastrophic adverse effect on operations, assets, or individuals.
Such an event could:		
• cause a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced, • result in minor damage to assets, • result in minor financial loss, or • result in minor harm to individuals.	• cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced, • result in significant damage to assets • result in significant financial loss, or • result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.	• cause a severe degradation in or loss of mission capability to an extent and duration the organization is not able to perform one of more of its primary functions, • result in major damage to assets, • result in major financial loss, or • result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

Who Determines Required Certification Level?

- The contracting agency should select the appropriate TX-RAMP level based on **confidentiality requirements** and the organizational **impact determination**.

- If a provider is seeking certification without contracting agency involvement, the provider can select the level.

- If level selection conflict exists across multiple contracting agencies, the provider should make the appropriate selection.

- Services certified at TX-RAMP Level 1 may request a TX-RAMP Level 2 assessment as circumstances necessitate.

Certification Requirements Timeline

- For cloud services that require Level 2 certification:
  - must be certified by **January 1, 2022,** to enter/renew contracts.

- For cloud services that require Level 1 certification:
  - must be certified by **January 1, 2023,** to enter/renew contracts.

- Cloud services granted TX-RAMP Provisional Certification
  - must obtain a TX-RAMP certification (or equivalent) within **18 months** from the date the provisional certification is granted.

- Existing contracts for cloud services **do not** need to be certified until renewed or new contract is executed.

Accepted Documentation/Evidence for Provisional Status

DIR will accept security-assessment/audit report documentation for review to determine whether provisional status may be granted.

- **Agency-sponsored request**
  - Notifies DIR of the assessment criteria used, date of assessment, impact level authorized, and additional relevant information if applicable.
  - Agency does not need to provide raw risk assessment results.
  - Common Assessments: HECVAT, CAIQ, CIS 18, TAC 202, SOC 2, 800-171, agency developed.

- **Third-party review request**
  - Provider completes assessment request form and notes the third-party review evidence.
  - DIR launches vendor portal questionnaire to collect documentation/evidence.
  - DIR reviews evidence and determines eligibility for provisional status.
  - Common Artifacts/Reports: SOC 2, ISO 27k, Regulatory Audits, CSA STAR, HITRUST, etc.

StateRAMP | FedRAMP

Existing/Accepted RAMP Statuses

- DIR will certify a cloud computing service under the corresponding impact level from accepted statuses of FedRAMP and StateRAMP using the FedRAMP Marketplace & StateRAMP Authorized Vendor List designations.

- **FedRAMP Marketplace:**
  - https://marketplace.fedramp.gov/#!/products?sort=productName

- **StateRAMP Authorized Vendor List:**
  - https://stateramp.org/vendor-list/

TX-RAMP | StateRAMP | FedRAMP

TX-RAMP	StateRAMP	FedRAMP
• Based on NIST 800-53r4	• Based on NIST 800-53r4	• Based on NIST 800-53r4
• Requires DIR Assessment	• Requires 3PAO Audit	• Required 3PAO Audit
• No cost	• Cost	• Cost
• Impact level determined by TAC 202	• Impact determined by classification tool	• Impact level determined by FIPS 199
• ConMon available to contracting agencies	• ConMon available to public sector members	• ConMon available to federal agencies
• Mandatory for state agencies	• Not mandatory	• Mandatory for federal executive agencies
• Does not require business w/ state	• 501c(6)	• Must do business with federal gov

TX-RAMP | StateRAMP | FedRAMP

TX-RAMP	StateRAMP	FedRAMP
Level 1	Category 1/1+	Low
Level 2	Category 3	Moderate
		High

Verified Offerings:
Certified

Verified Offerings:
Ready, Authorized, Provisional

Verified Offerings:
Ready, P-ATO, ATO (Authorized)

Progressing Offerings:
In Process, Pending

Progressing Offerings:
Active, In Process, Pending

Progressing Offerings:
In Process

TX-RAMP Assessment

Assessment Initiation

- A state agency may submit a request for assessment of a cloud service directly into SPECTRIM and sponsor the request if the required cloud provider information is available.

- A vendor may also initiate a request for assessment without agency sponsorship. Further, a state agency may request or require a vendor with whom they intend to contract with for cloud services to complete the **TX-RAMP assessment request form.**

- DIR will import the request form information into SPECTRIM. Agencies may then elect sponsor the request for assessment to assist in assessment review prioritization.

Assessment Request – Information Needed

- CSP Contact Information
- DIR Contract Information, if applicable
- Cloud Service Name/Description/URL
- Cloud Service Manufacturer
- Cloud Service Model/Deployment Model
- Procurement Information
- Requested Assessment Level
- Requested Assessment Initiation Date
- Number of State Entities Leveraging Cloud Service

https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact

Assessment Prioritization

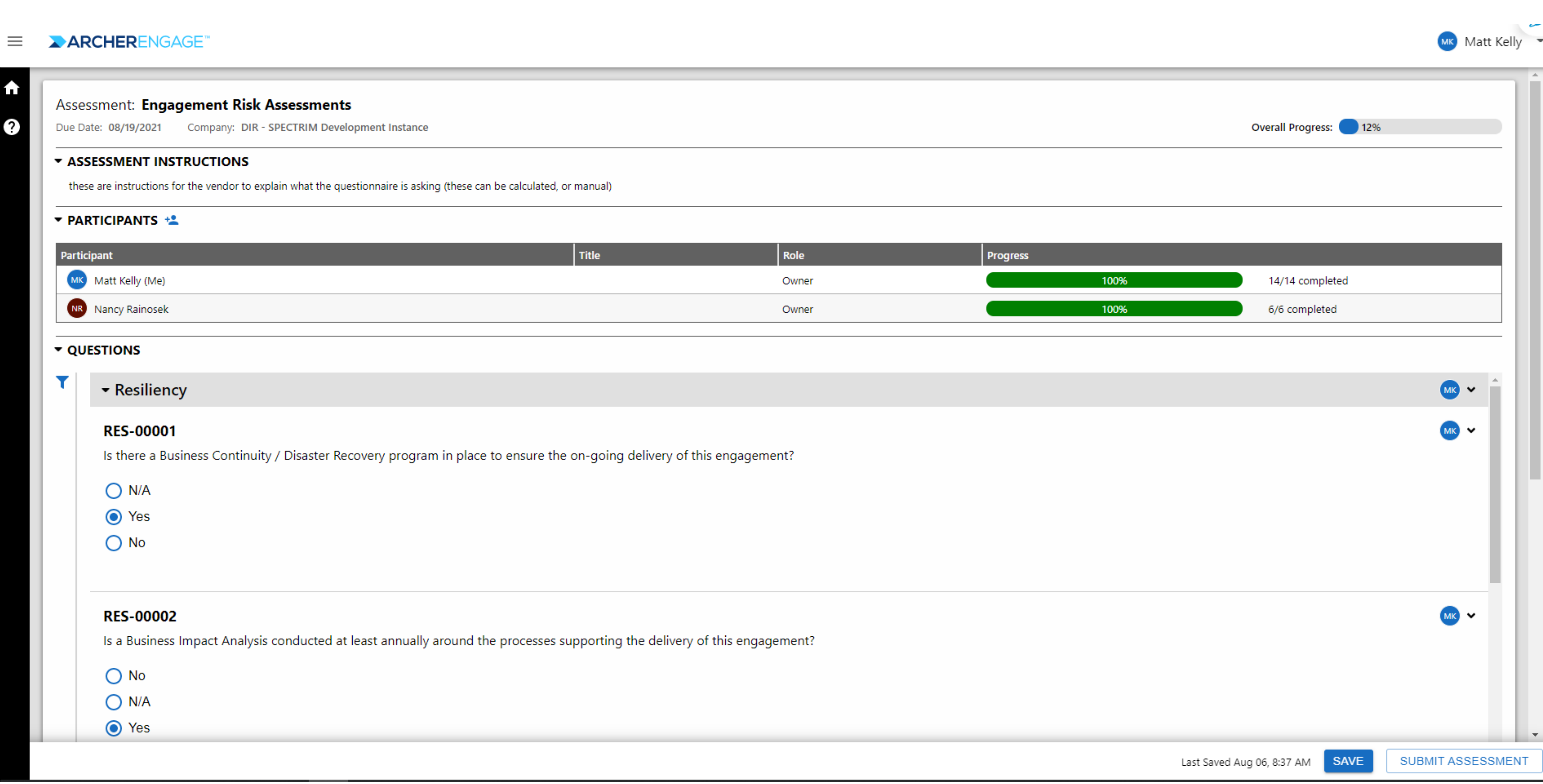
DIR will review assessments in the order that they are received. Priority will be granted to those assessments sponsored by a state agency, even if the vendor initiates the process. DIR may also consider additional factors in determining the priority of an assessment including, but not limited to:

- level of certification requested
- existing authorizations or certifications
- state agency described priority or justification
- existing and planned procurement activities

Controls Assessment

TX-RAMP Level	Number of Controls/Enhancements Assessed
Level 1	**124**
Level 2	**325**

CONTROL FAMILY	TX-RAMP LEVEL 1	TX-RAMP LEVEL 2
ACCESS CONTROL	11	43
AUDIT AND ACCOUNTABILITY	10	19
AWARENESS AND TRAINING	4	5
CONFIGURATION MANAGEMENT	8	27
CONTINGENCY PLANNING	6	24
IDENTIFICATION AND AUTHENTICATION	15	27
INCIDENT RESPONSE	8	18
MAINTENANCE	4	11
MEDIA PROTECTION	4	10
PERSONNEL SECURITY	8	8
PHYSICAL AND ENVIRONMENTAL PROTECTION	9	20
PLANNING	3	6
RISK ASSESSMENT	4	10
SECURITY ASSESSMENT AND AUTHORIZATION	8	15
SYSTEM AND COMMUNICATIONS PROTECTION	8	32
SYSTEM AND INFORMATION INTEGRITY	7	28
SYSTEM AND SERVICES ACQUISITION	7	22
TOTAL	**124**	**325**



Assessment: **Engagement Risk Assessments**

Due Date: 08/19/2021 Company: DIR - SPECTRIM Development Instance

Overall Progress: 12%

ASSESSMENT INSTRUCTIONS

these are instructions for the vendor to explain what the questionnaire is asking (these can be calculated, or manual)

PARTICIPANTS

Participant	Title	Role	Progress
MK Matt Kelly (Me)		Owner	100% 14/14 completed
NR Nancy Rainosek		Owner	100% 6/6 completed

QUESTIONS

Resiliency

RES-00001

Is there a Business Continuity / Disaster Recovery program in place to ensure the on-going delivery of this engagement?

○ N/A
● Yes
○ No

RES-00002

Is a Business Impact Analysis conducted at least annually around the processes supporting the delivery of this engagement?

○ No
○ N/A
● Yes

Vendor Portal Questionnaire

- Launched questionnaires can be assigned delegates to questions, sections, or the entire questionnaire provided the delegate **has the same email domain as the original recipient of the assessment.**

- If a delegate with a different domain needs access, they will either need to coordinate responses with the original recipient, or a new questionnaire will need to be launched to the appropriate domain contact.

General Assessment Information

- Responses should be truthful, accurate, and reflect current state.
- Answering “no” to a question doesn’t mean you will be disqualified.
- Leverage the open text fields for each family to provide additional relevant information you want considered.
- Make sure you keep contact information up to date.
- Documentation should fully address applicable control requirements.

Required Documentation

#	TX-RAMP DOCUMENTATION REQUIREMENTS
1	BOUNDARY & DATA FLOW DIAGRAM
2	ROLES & PERMISSIONS MATRIX
3	INCIDENT RESPONSE PLAN
4	SYSTEM SECURITY PLAN
5	INFORMATION SYSTEM CONTINGENCY PLAN
6	CONFIGURATION MANAGEMENT PLAN
7	SECURITY POLICY - ACCESS CONTROL (AC)
8	SECURITY POLICY - AWARENESS AND TRAINING (AT)
9	SECURITY POLICY - AUDIT AND ACCOUNTABILITY (AU)
10	SECURITY POLICY - SECURITY ASSESSMENT AND AUTHORIZATION (CA)
11	SECURITY POLICY - CONFIGURATION MANAGEMENT (CM)
12	SECURITY POLICY - CONTINGENCY PLANNING (CP)
13	SECURITY POLICY - IDENTIFICATION AND AUTHENTICATION (IA)
14	SECURITY POLICY - INCIDENT RESPONSE (IR)
15	SECURITY POLICY - MAINTENANCE (MA)
16	SECURITY POLICY - MEDIA PROTECTION (MP)
17	SECURITY POLICY - PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)
18	SECURITY POLICY - PLANNING (PL)
19	SECURITY POLICY - PERSONNEL SECURITY (PS)
20	SECURITY POLICY - RISK ASSESSMENT (RA)
21	SECURITY POLICY - SYSTEM AND SERVICES ACQUISITION (SA)
22	SECURITY POLICY - SYSTEM AND COMMUNICATIONS PROTECTION (SC)
23	SECURITY POLICY - SYSTEM AND INFORMATION INTEGRITY (SI)

Suggested Templates

https://stateramp.org/templates-resources/

Documentation

Category	Description
Compliance	•Documentation provides sufficient and complete evidence of the control requirements satisfaction.
Clarity	•Correct and consistent format •Correct and continuous section numbering •Logical presentation of material •Current dates and timely content •Non-standard terms, phrases, acronyms, and abbreviations defined •Proper titles and labels on figures •No ambiguous statements or content •Minimal and appropriate use of the passive voice •No awkward phrases, typographical errors, spelling errors, missing words, or incorrect page and section numbers •Reasonable sentence and paragraph lengths •Use of generally accepted rules of grammar, capitalization, punctuation, symbols, and notation •Appropriate and accurate identification of cross-references •Figure text is readable; figure graphics are sharp
Completeness	•Responsive to all applicable requirements •Indicate compliance with applicable requirements •Includes all appropriate sections of documentation requested •Includes all attachments and appendices •Includes table of contents, list of tables, and list of figures if applicable •Figures include required information, correct labels, and keys to color/line formats
Conciseness	•Content and complexity are relevant to the audience •No superfluous words or phrases
Consistency	•Terms have the same meaning throughout the document •Items are referred to by the same name or description throughout the document •The level of detail and presentation style are the same throughout the document •The material does not contradict predecessor documents •All material is subsequent documents has a basis in the predecessor document •Figure content agrees with text

System Security Plan (SSP)

Key Components

- Information System Info
- Categorization
- Key Roles
- Cloud Info
- User/Roles
- Network Architecture
- Data Flow
- PPS
- System Interconnections
- Minimum Security Controls

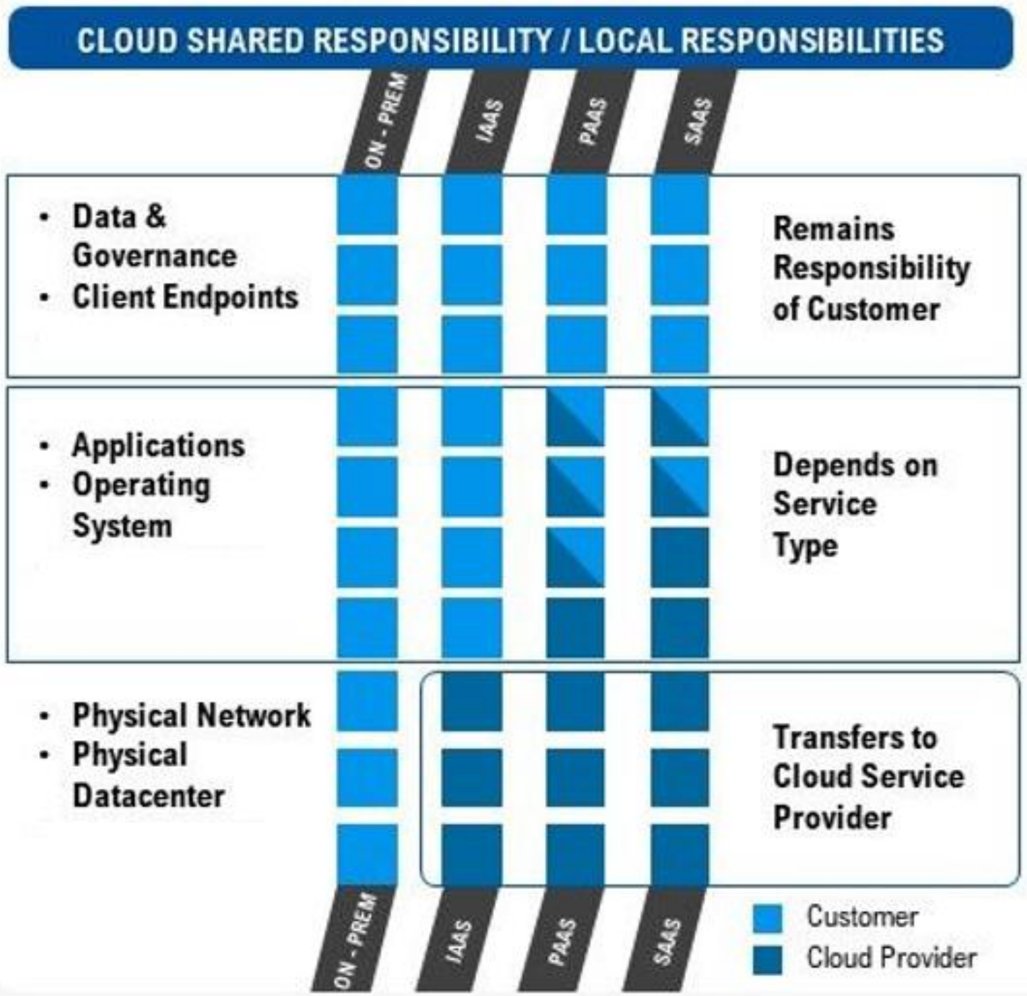
Attachments

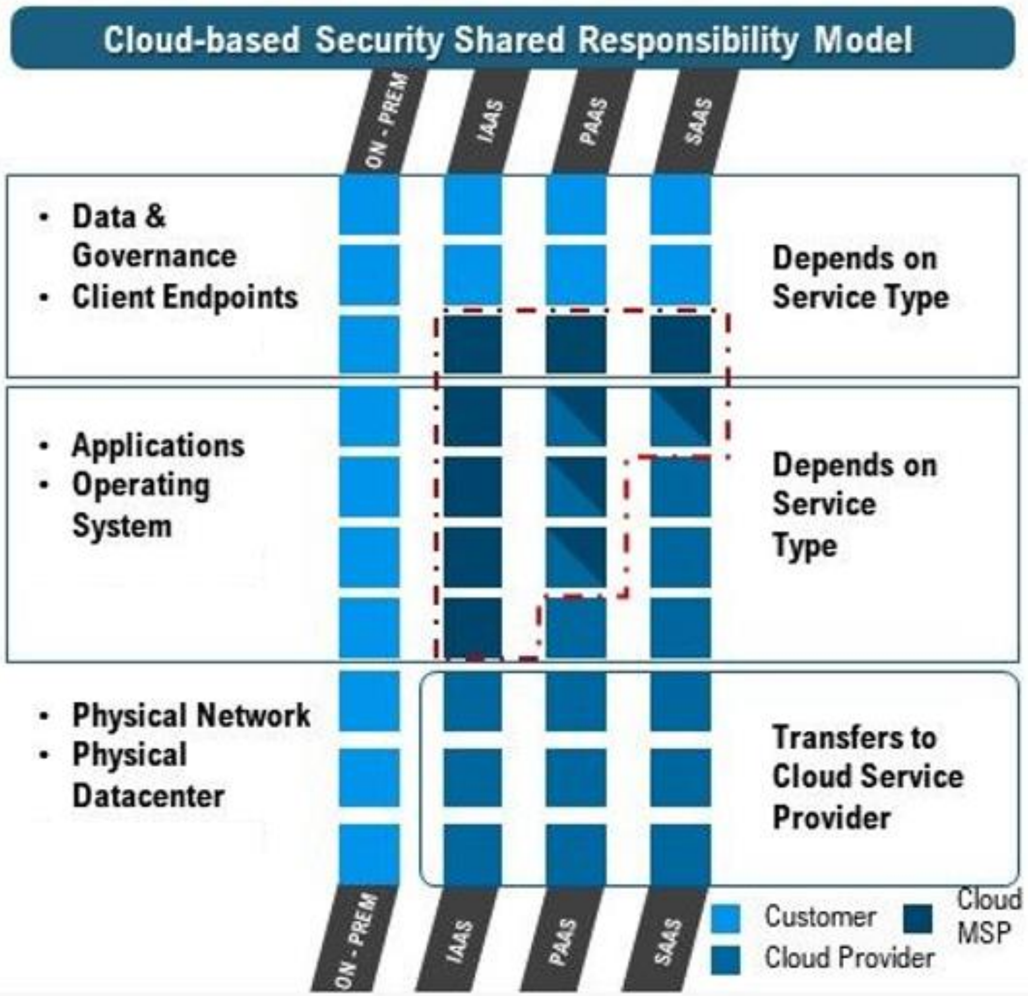
- Control Implementations
- CIS Matrix
- Inventory Workbook
- Laws & Regulations
- Policies
- Config Mgmt. Plan
- Contingency Plan
- IR Plan
- Rules of Behavior
- Separation of Duties Matrix

General Policy/Procedures Requirements

- **Policies need to address:**
  - Purpose
  - Scope
  - Roles
  - Responsibilities
  - Management commitment
  - Coordination among organizational entities
  - Compliance
- **Policy Review/Update at least every three (3) years.**
- **Procedure Review/Update at least annually.**
- **Identify Personnel/Roles to whom policies/procedures are disseminated.**

Shared Responsibility Model



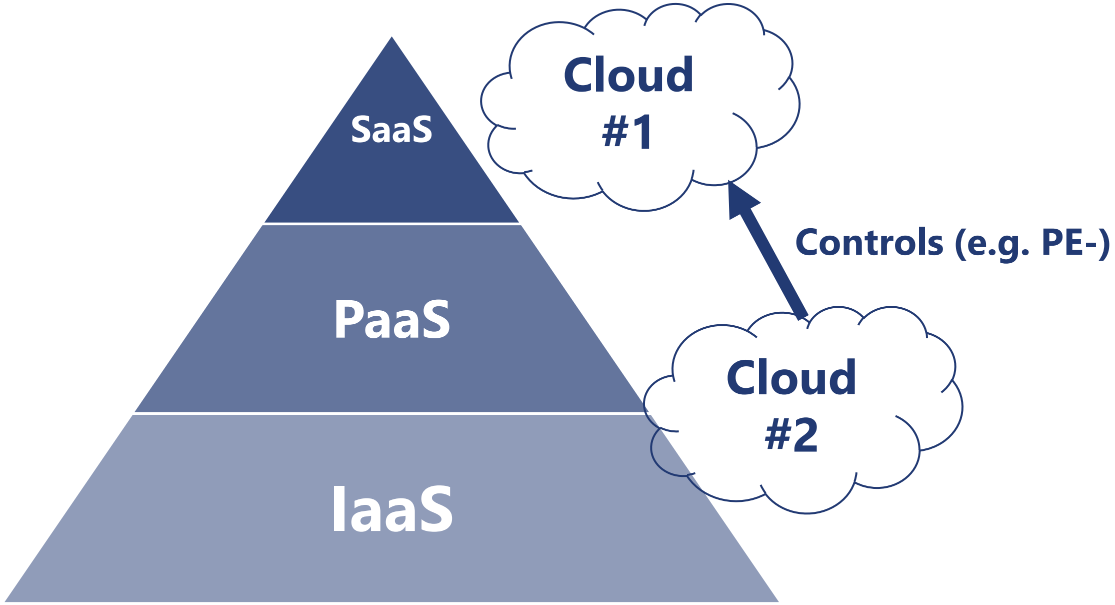


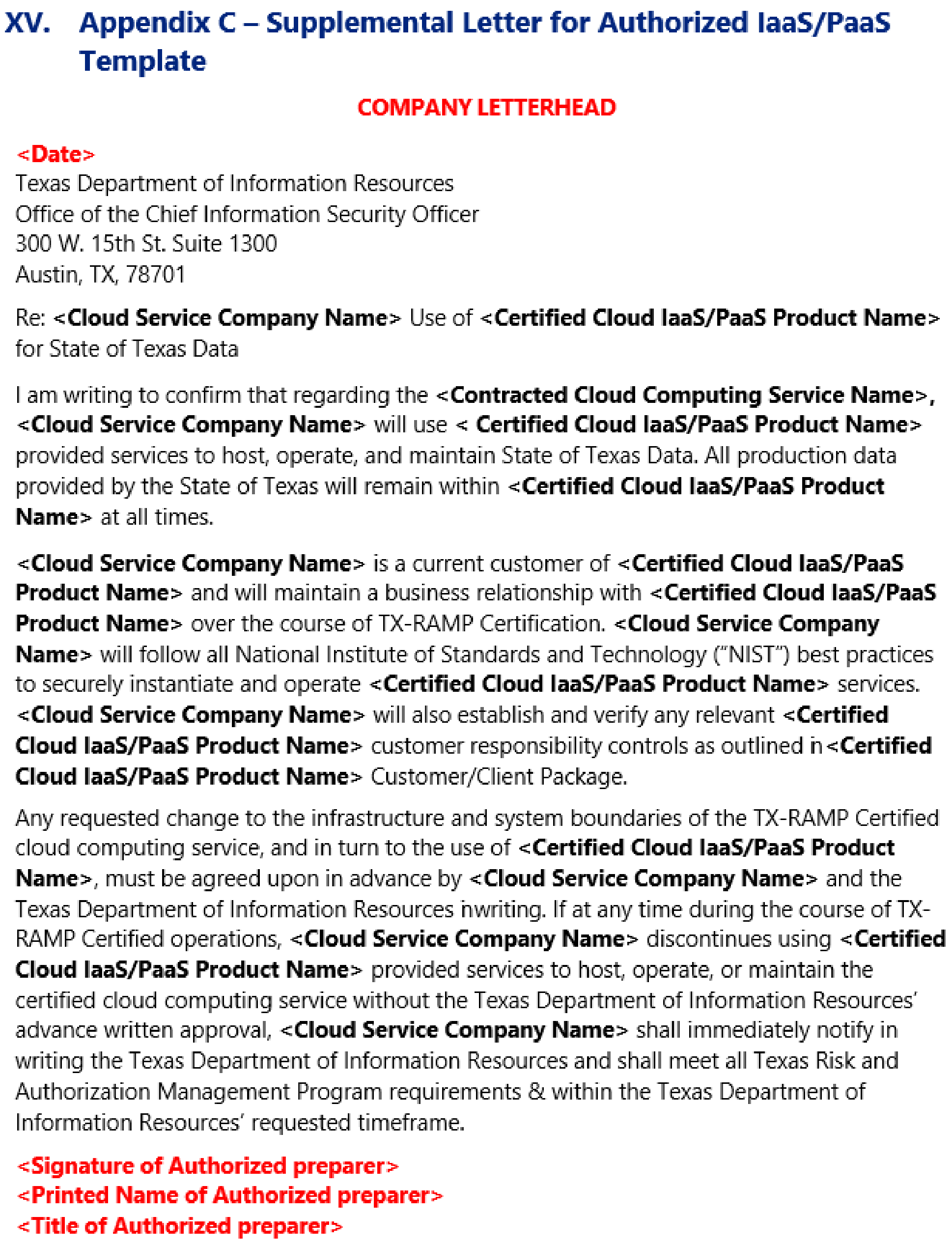
**~~~Service configuration – customer always responsible~~~**

Leveraging Authorizations

- SaaS providers may inherit IaaS/PaaS controls through operating on certified cloud services.

- Need to complete the supplemental letter and submit with assessment.





XV. Appendix C – Supplemental Letter for Authorized IaaS/PaaS Template

COMPANY LETTERHEAD

<Date>
Texas Department of Information Resources
Office of the Chief Information Security Officer
300 W. 15th St. Suite 1300
Austin, TX, 78701

Re: <**Cloud Service Company Name**> Use of <**Certified Cloud IaaS/PaaS Product Name**> for State of Texas Data

I am writing to confirm that regarding the <**Contracted Cloud Computing Service Name**>, <**Cloud Service Company Name**> will use < **Certified Cloud IaaS/PaaS Product Name**> provided services to host, operate, and maintain State of Texas Data. All production data provided by the State of Texas will remain within <**Certified Cloud IaaS/PaaS Product Name**> at all times.

<**Cloud Service Company Name**> is a current customer of <**Certified Cloud IaaS/PaaS Product Name**> and will maintain a business relationship with <**Certified Cloud IaaS/PaaS Product Name**> over the course of TX-RAMP Certification. <**Cloud Service Company Name**> will follow all National Institute of Standards and Technology ("NIST") best practices to securely instantiate and operate <**Certified Cloud IaaS/PaaS Product Name**> services. <**Cloud Service Company Name**> will also establish and verify any relevant <**Certified Cloud IaaS/PaaS Product Name**> customer responsibility controls as outlined in<**Certified Cloud IaaS/PaaS Product Name**> Customer/Client Package.

Any requested change to the infrastructure and system boundaries of the TX-RAMP Certified cloud computing service, and in turn to the use of <**Certified Cloud IaaS/PaaS Product Name**>, must be agreed upon in advance by <**Cloud Service Company Name**> and the Texas Department of Information Resources inwriting. If at any time during the course of TX-RAMP Certified operations, <**Cloud Service Company Name**> discontinues using <**Certified Cloud IaaS/PaaS Product Name**> provided services to host, operate, or maintain the certified cloud computing service without the Texas Department of Information Resources' advance written approval, <**Cloud Service Company Name**> shall immediately notify in writing the Texas Department of Information Resources and shall meet all Texas Risk and Authorization Management Program requirements & within the Texas Department of Information Resources' requested timeframe.

<Signature of Authorized preparer>
<Printed Name of Authorized preparer>
<Title of Authorized preparer>

Continuous Monitoring

Continuous Monitoring Reporting

- **Vulnerability Reporting**
  - Level 1 – Annual
  - Level 2 – Quarterly
- **Critical Security Issues**
  - As needed (48 hours)
- **Breach of Confidential/PII**
  - As needed (48 hours)
- **Significant Changes**
  - As needed (30 days)

CVSS Severity	Reporting Components
Low (0.1-3.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities
Medium (4.0-6.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities
High (7.0-8.9)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities •Planned/Current Remediation Activities/Compensating Controls
Critical (9.0-10.0)	•Number Identified During Reporting Period •Number Remediated During Reporting Period •Number of Existing Vulnerabilities •Planned/Current Remediation Activities/Compensating Controls

Continuous Monitoring Reporting

- Continuous Monitoring reporting reminders will be sent to identified points of contact on a regular basis (quarterly/annual)

- Reminders will contain link to the continuous monitoring questionnaire.

- Cloud provider will complete the questionnaire and note any additional relevant information.

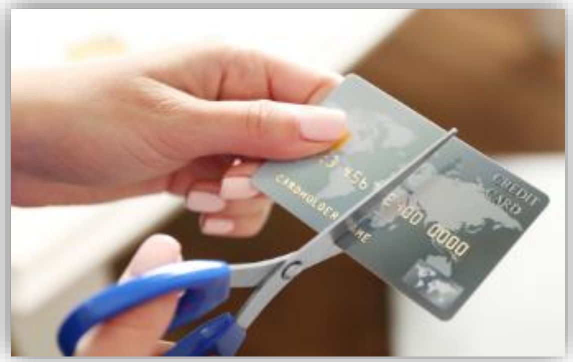
- Questionnaire information will be populated in SPECTRIM and available for agency review for agencies contracting for the service.

Additional Information

Certification Revocation

Events that may result in a revocation include (not limited to) the following:

- Failure of a vendor to maintain baseline compliance with TX-RAMP requirements.
- Failure to inform parties in a timely manner of significant changes to the cloud offering.
- Failure to inform required parties of the loss of other accepted RAMP certification.
- Failure to provide required continuous monitoring documents.
- The report of false or misleading information to DIR or a state agency.
- Referencing non-certified cloud computing services as TX-RAMP certified.
- Failure to report a breach of system security to DIR within 48 hours of discovery.



Grievance/Appeals

- Agencies may report perceived failures to maintain compliance
- Providers may appeal certification decisions
- Notification of grievance appeals must be submitted to tx-ramp@dir.texas.gov in writing
- DIR determines corrective/remediation/revocation actions

Re-certification

- TX-RAMP Level 1 and Level 2 certifications are **valid for three (3) years** from the date the last certification was conferred upon a cloud computing service, provided that the vendor is compliant with the program requirements enumerated in this Program Manual.

- Recertification requires the vendor to review and update control implementation details as necessary and provide updated documentation to DIR for review.

- The identified points of contact for vendors with TX-RAMP certified cloud computing services will be notified by automated email at 12 months and 6 months prior to the certification end date. This email will include instructions for completing the recertification process.

Information Sessions

Overview Tuesday 11/16 1:00-2:30PM (agencies)

https://www.zoomgov.com/webinar/register/WN_qNN6aBNBR36KbU28bx3_cQ

Overview Friday 11/19 9:00-10:00AM (vendors)

https://www.zoomgov.com/webinar/register/WN_C-M60E-ISUKAscXEjNExqw

SPECTRIM Overview/Training

TBD

Contact tx-ramp@dir.texas.gov

Q & A

Thank You – tx-ramp@dir.texas.gov

dir.texas.gov

#DIRisIT

@TexasDIR

Transforming How
Texas Government
Serves Texans

Texas Department of Information Resources